

# Release Notes for McAfee® VirusScan® Enterprise 8.7i Patch 2

Thank you for using McAfee VirusScan Enterprise software version 8.7i Patch 2. This document contains important information about this release. We strongly recommend that you read the entire document.

## Contents

- Purpose
- Rating
- Improvements
  - Previous Improvements
- Known Issues
- Resolved Issues
  - Patch 2 resolved issues
  - Patch 1 resolved issues
- Installation instructions
  - Verifying installation
  - Removing the patch
- License attributions

## About this release

- Patch Release: 08-31-2009

This release was developed for use with:

- VirusScan Enterprise: 8.7i
- Detection Definitions (DAT): 5700.0000
- Scan Engine: 5.3.01

Make sure you have installed the correct version of the product(s) in this list before using this release.

\*This document makes references to the following products as *VirusScan Modules*:

- McAfee® VirusScan® Enterprise for Offline Virtual Images 1.0
- McAfee® VirusScan® Enterprise for Offline Virtual Images 2.0
- McAfee® VirusScan® Enterprise for use with SAP NetWeaver® platform 1.0
- McAfee® VirusScan® Enterprise for Storage 1.0

## Purpose

This document supplements the product Release Notes in the release package and details fixes included in VirusScan Enterprise 8.7i Patch 2.

This Patch contains a variety of improvements. McAfee has spent a significant amount of time finding, fixing, and testing the fixes in this release. Please review the Known and Resolved Issues lists for additional information on the individual issues. Refer to online KnowledgeBase article KB66795 at <http://knowledge.mcafee.com> for the most current information regarding this release.

## Rating

McAfee recommends this release for all environments. Patch 2 is considered a *High Priority Release*. See McAfee Support KnowledgeBase article KB51560 for information on ratings.

## Improvements

This release of the software includes the following improvements.

1. Improvements were made to the way that the CommonShell scanner interacts with file I/O. This improves performance with on-access scanners within the product.
2. VirusScan Enterprise 8.7i Patch 2 now has the ability to report compliance to the newer versions of Windows Security Center.
3. The VirusScan Enterprise 8.7i extension has improved support for ePolicy Orchestrator 4.5 with Firefox 3.0 and Internet Explorer 8.0.
4. Several modifications were made to the way that VirusScan Enterprise's system tray icon interacts with the new functionality of McAfee Agent 4.5.
5. The file extension .txt was added to the SmoothWritesExtension registry value to increase performance in handling text files.
6. Russian language support was added to the VirusScan Enterprise user interface, NAP file, and extension.

**NOTE:** See items #3 and #4 under *Known Issues* for further information about this topic.

## Previous Improvements

Previous releases of the software include the following improvements.

1. The VirusScan Reports extension now has updated queries to show the status of Artemis settings for the on-access, on-demand, and email scanners.

**NOTE:** The Artemis status requires VirusScan Enterprise 8.5i Patch 8 or VirusScan Enterprise 8.7i Patch 1 to be installed on the client systems, in order to correctly populate the reports. Refer to McAfee Support KnowledgeBase article KB53732 for further information on Artemis functionality.

2. On-Access Scanner's Artemis level setting is now modifiable via the properties UI, and the equivalent VirusScan 8.7i NAP and Extension included in the patch package.

**NOTE:** Because this setting is new with this release of the VirusScan 8.7i NAP and extension, there is no preserved setting upon check-in of the management package. The ePolicy Orchestrator administrator will need to update that setting in the policies to match the current Artemis policy.

3. Several modifications have been made to the way VirusScan Enterprise interacts with the operating system on startup, suspend, and shutdown. These modifications resolve and improve performance issues.
4. Current DAT files are compressed to conserve network bandwidth. Now, changes have been made to decompress the DATs during the AutoUpdate process and leave them in that state, so that scanners do not have to decompress them during initialization of the scan.
5. The on-demand scanner now uses Windows Priority Control setting for the scan process. This lets the operating system set the amount of CPU time that the on-demand scanner receives at any point in the scan process. The System Utilization setting in the On-Demand Scan Properties maps to Windows Priority Control as:

Utilization	Priority
10%	Low
20%-50%	Below Normal
60%-100%	Normal

6. The on-access, on-demand, email, and script scanners now use a runtime copy of the DATs. This change has reduced the memory consumption of affected scanners by having the DATs in a readily available state for the scan engine to load.

**NOTE:** In some scenarios, the runtime DATs are not available. See item #1 under *Known Issues*. Refer to

McAfee Support KnowledgeBase article KB65459 for further information on runtime DATs.

7. VirusScan Enterprise functions that request the current version of DATs no longer need to initialize the scan engine to do so. This prevents excessive CPU spikes during ePolicy Orchestrator properties collection, as well as other areas that poll the DATs.
8. The on-access scanner memory scan function (Processes on enable) has been modified significantly to make it more comprehensive.

**NOTE:** The improved functionality can cause a performance impact to the system. See item #2 under *Known Issues*.

9. When a web browser opens a site that is script-intensive, scanning the scripts adds to the delay of loading the page. This Patch contains new functionality for ScriptScan whitelisting. If the web site is a trusted Intranet and/or frequently visited, the new implementation now allows for the exclusion of that the site from script scanning.

**NOTE:** Refer to McAfee Support KnowledgeBase article KB65382 for further information.

10. The installation packages for patches and reposts have been upgraded so that the installation log name, created in the McAfeeLogs folder, has a dynamically generated name based on the current date and time of the installation. This helps save logs that might have been overwritten with the previous "backup previous log only" method.

## Known issues

Known issues in this release of the software are described below:

1. **Issue:** In some situations, the product switches over to using the normal copy of the DAT files, instead of the runtime DATs:
  - If the McAfee AntiSpyware Enterprise module is installed after VirusScan Enterprise 8.7i Patch 1 is on the system, some of the new registry settings, which are new for the runtime functionality, were changed back. This resolves itself with a restart of the McTaskManager service or with a reboot.
  - If one of the scanners is busy on a large file when the AutoUpdate process posts the revised copy of the DATs, the process of refreshing the runtime copy of the DATs times out. All scanners use the normal DATs until the next successful update.
  - The VirusScan Modules\* will not use the runtime DAT functionality until they received their next Patch.
2. **Issue:** With the improved functionality of the on-access scanner memory scan, lower and middle ranged systems may see a performance impact at startup and after a successful AutoUpdate of the engine or DATs. Currently the Process on enable option is enabled by default on the shipping version of VirusScan Enterprise 8.7i. McAfee recommends that in a managed environment, disable this option prior to deployment of the Patch, until the impact of memory scanning can be determined for your environment. It is not possible to maintain both the more comprehensive scanning that comes with Patch 1 and later, and the former level of scanning. Therefore, only the more comprehensive scan is used.

### NOTE FOR CURRENT AND NEW USERS:

- The Patch installation does not modify current settings to disable the *Process on enable* option.
  - The VirusScan 8.7i NAP and extension that are included with the Patch do change the McAfee Default policy, but do not modify the My Default policy, or any custom policy settings that were made prior to the checkin of the new NAP/extension.
  - The VirusScan Enterprise 8.7i Repost with Patch now installs with the *Process on enable* option disabled, unless the Maximum Security option is selected during the installation.
3. **Issue:** With the introduction of support for Russian, you might need to remove the previous version of the extension from ePolicy Orchestrator before adding the new extension. If you do not, some of the interface might be displayed in the original language.
  4. **Issue:** McAfee Agent 4.0 Patch 2 and later include support for displaying status and logs in Russian. Older versions display this information in English by default.
  5. **Issue:** Since VirusScan Enterprise 8.7i Patch 2 and later include the new interface for reporting status to Windows Security Center, uninstalling the Patch removes this function -- without reintroducing the older

expired function. This means that Windows Security Center does not report VirusScan Enterprise 8.7i being installed until Patch 2 or later is implemented.

6. **Issue:** When you remove the McAfee AntiSpyware Module, the status in Windows Security Center is not updated.
7. **Issue:** In deployments of VirusScan Enterprise 8.7i Patch 2 with McAfee Agent 4.5, the VirusScan tray plug-in does not appear until after a restart of the McAfee system tray icon. If VirusScan is uninstalled, the VirusScan tray plug-in is still visible until a similar restart.
8. **Issue:** This Patch adds needed support for McAfee VirusScan Enterprise for Offline Virtual Images 2.0, and should not be removed unless the VirusScan Module is removed first.
9. **Issue:** The Patch installer included an MSI deferred action to resolve an issue found when attempting to uninstall the Patch on some newer operating systems. The deferred.mfe file updated the cached MSI of the currently installed VirusScan 8.7i product. If the Patch is included in a McAfee Installation Designer customized package, the deferred.mfe file was not included, and therefore the Patch might not be able to be uninstalled in some newer operating systems.
10. **Issue:** If you installed this release interactively and cancelled the installation on a system where a previous Patch was installed, after the rollback was complete, the previous Patch might no longer reported to ePolicy Orchestrator or appeared in the *About VirusScan Enterprise* window.
11. **Issue:** Installing the Patch and specifying a log file path using the Microsoft Installer (MSI) switch "/L" did not log to the specified path. A log file capturing full data was logged to the folder "McAfeeLogs" under the Temp folder.
12. **Issue:** If Host Intrusion Prevention 6.x or later was installed and disabled prior to installing VirusScan Enterprise, it was necessary to re-enable Host Intrusion Prevention and disable it again, in order for VirusScan Buffer Overflow Protection to be properly enabled.
13. **Issue:** Uninstalling VirusScan Enterprise Patches is possible for computers running Windows Installer v3.x or later. This technology is not fully integrated for Windows 2000 operating systems, so there is no option to remove the Patch in Add/Remove programs. See instructions under Removing the Patch for removal via command-line options.
14. **Issue:** Patches for VirusScan Enterprise 8.7i can only be uninstalled via Add/Remove programs, not via ePolicy Orchestrator.

## Resolved issues

The resolved issues are divided into subsections per patch, showing when each fix was added to the compilation.

### Patch 2 resolved issues:

1. **Issue:** Processes that ended were still listed in Task Manager. (Reference: 482720)  
**Resolution:** The link driver no longer retains the handles to processes that have closed.
2. **Issue:** On a system using large quantities of handles, particularly busy servers, VirusScan would cache excessive amounts of data in non-paged pool memory. (Reference: 492541)  
**Resolution:** The link driver has been updated to reduce the amount of overhead in the data used for operations.
3. **Issue:** In high I/O environments where Access Protection is enabled, a performance degradation symptom could be encountered, appearing as a hang. Internal processing by VirusScan drivers occurred serially, contributing to a bottleneck when large volumes of I/O were filtered. (Reference: 497580)  
**Resolution:** The link and mini-firewall drivers no longer cause a sequential release of objects containing gathered information on the I/O request. This should increase performance on multi-processor environments.
4. **Issue:** The setting in Email Scan for Heuristic network check for suspicious files was not being updated based on the user interface or policy changes. (Reference: 493594)

**Resolution:** The setting now updates the proper registry location to reflect the change in the user interface.

5. **Issue:** To support ePolicy Orchestrator's Countermeasures functionality, the properties collection was modified for the new data. The section title was not named correctly to reflect the new functionality. (Reference: 487603)  
**Resolution:** The section in the computer properties was updated to Countermeasures for ePolicy Orchestrator to use the data properly.
6. **Issue:** On systems with Symantec's SVS Client software installed, the on-access scan features did not load. (Reference: 441670)  
**Resolution:** The On-Access Scanner service now communicates with our filter drivers on systems where SVS Client software is installed.
7. **Issue:** The Patch installer registered ScriptScan libraries, even when the user interface had the feature set as disabled. (Reference: 498347)  
**Resolution:** The Patch installer no longer runs the ScriptScan registration function, in order to prevent the setting from being changed.
8. **Issue:** When Access Protection and Buffer Overflow were disabled in an attempt to improve performance, the drivers were still loaded, although not active, causing little change in performance. (Reference: 465506)  
**Resolution:** Disabling the Access Protection and Buffer Overflow drivers now yields the expected performance increase.
9. **Issue:** The on-access scanner did not properly time out when scanning large archives. This could lead to the system failing to copy files. (Reference: 464768)  
**Resolution:** The on-access scanner service now successfully times out at the interval specified in the user interface.
10. **Issue:** When the on-delivery Outlook scanner received emails to scan, some keyboard entries could be lost. (Reference: 480992)  
**Resolution:** The Outlook scanner now handles the on-delivery scan of an email with Microsoft Outlook 2007, and caches the keys entered during that time.
11. **Issue:** When VirusScan Enterprise 8.7i was installed on a system running Windows 2008, uninstall fails. (Reference: 496609)  
**Resolution:** The Microsoft Patch (MSP) installer corrects a custom action that was preventing the re-enabling of Microsoft Windows Defender.
12. **Issue:** When VirusScan Enterprise 8.7i is installed on a system running Windows 2000, where the installation was customized using McAfee Installation Designer, a subsequent patch update might fail to install. (Reference: 489712)  
**Resolution:** The MSP installer modifies the cached MSI for VirusScan Enterprise 8.7i, on Windows 2000, in order to correct the source of failure.
13. **Issue:** Silent installations might fail on hard drives that are designated as dynamic. The on-access scanner service fails to start, and the installation rolls back. (Reference: 443669)  
**Resolution:** The Patch 1 Repost and later installation packages now install to a dynamic disk, silently.

## Patch 1 resolved issues:

1. **Issue:** An unauthenticated remote denial-of-service attack was discovered. (Reference: 470184)  
**Resolution:** The product no longer allows the denial-of-service attack.
2. **Issue:** Under certain conditions, the Lotus Notes scanner of VirusScan Enterprise can mistakenly deny access to the Lotus Notes internal processes, if a note was being accessed more than once. (Reference: 438541)  
**Resolution:** The Lotus Notes scanner has been adjusted to better handle re-entrance scanning of the same note.
3. **Issue:** Silent installs may fail on hard drives that are designated as dynamic. The on-access scanner service fails to start, and the installation will roll back. (Reference: 443669)  
**Resolution:** The patch 1 and later install packages will now install to a dynamic disk, silently.
4. **Issue:** Sporadic crashes were seen on multi-processor systems, with the Lotus Notes scanner file

ncdaemon.exe, during startup and general use of Lotus Notes. (Reference: 442337)

**Resolution:** The Lotus Notes scanner has been corrected to prevent a race condition where different scanner threads were starting and stopping out of sequence.

5. **Issue:** A 8E bugcheck (blue screen) sometimes occurred when VirusScan Enterprise 8.7i was installed along with Checkpoint VPN-1 SecureClient. (Reference: 438771)

**Resolution:** The link driver was updated to avoid probing kernel memory unnecessarily.

**NOTE:** For this fix to prevent the above issue, the files need to be placed on the system during the installation of VirusScan Enterprise, before the services start. The repost of VirusScan Enterprise 8.7i with Patch 1 will be needed to see the resolution.

6. **Issue:** A flaw in the caching algorithm sometimes caused files in removable media to not be scanned. (Reference: 443104)

**Resolution:** The Anti-Virus Filter driver was updated to clear the cache of removable media upon attaching to the system.

7. **Issue:** The on-access scanner contained a flaw in the scan on close logic. This could cause a file to be queued up for scanning a second time. (Reference: 434475)

**Resolution:** The Anti-Virus Filter driver no longer queues these unnecessary scan requests.

8. **Issue:** During an upgrade from a customized VirusScan Enterprise 8.5i to VirusScan Enterprise 8.7i, An issue sometimes occurred where the configuration tool did not properly backup and restore the registry information. The installation was left in a state where some of the product information still showed as the older version. (Reference: 443019)

**Resolution:** The McAfee Installation Designer configuration applicator has been changed to be more comprehensive in backing up and in version checking during the upgrade, in order to prevent failures by other McAfee product installations that require version 8.7i.

**NOTE:** For this fix to prevent the above issue, the files need to be placed on the system during the installation of VirusScan Enterprise, before the services start. The repost of VirusScan Enterprise 8.7i with Patch 1 will be needed to see the resolution.

9. **Issue:** On Microsoft Windows Vista SP1 or 2008 server, sharing violations could occur when working with remote files while network drive scanning was enabled. This resulted in being denied access to files, or being unable to modify or save a file. (Reference: 447282)

**Resolution:** The Anti-Virus Filter driver has been updated to better handle potential sharing violations that could occur and avoid conflicts.

10. **Issue:** Prolonged use of the VirusScan Console was causing delays in loading subsequent loading of the Console window. (Reference: 456831)

**Resolution:** The VirusScan Console plug-in was corrected to properly clean up the .tmp files it creates at load time.

11. **Issue:** Access Protection rules were being triggered during creation of a VirusScan customized installation package via McAfee Installation Designer. This could lead to a crash of the McAfee Installation Designer tool. (Reference: 435728)

**Resolution:** The VirusScan Email Scan library appropriately handles the new Sensitivity level setting when it is displayed in the McAfee Installation Designer window.

12. **Issue:** Certain detections with multiple infections or clean actions were logging the action two times. One entry was made during the middle of the process, and the other during the final resolution. (Reference: 404787)

**Resolution:** The Common Shell scanner has been updated to report only the final resolution of the detection.

13. **Issue:** A 8E bugcheck (blue screen) might occur during the "Memory for Rootkits" portion of an on-demand scan. (Reference: 445490)

**Resolution:** The code analysis driver now uses a more robust method of querying the system for driver object data.

14. **Issue:** Access Protection block rules that were created for USB devices sometimes did not handle removing and reinserting the device multiple times. (Reference: 457415)

**Resolution:** The Access Protection, Anti-Virus Filter, and Link drivers have been updated to better handle reinserting the device.

15. **Issue:** The on-access scanner was not properly utilizing the *Scan files opened for Backup* option. (Reference: 457416)  
**Resolution:** The Anti-Virus Filter driver has been rectified to properly interpret the flag being sent from the on-access scanner.
16. **Issue:** In an ePolicy Orchestrator managed environment, the agent's Collect and Send Properties function could cause the McAfee Product Manager service to spike its CPU utilization for extended periods of time. (Reference: 457421)  
**Resolution:** The VirusScan Management Plug-in has been updated to call for the scan engine and DAT files via a new API call, rather than initializing the engine to retrieve the information. This lessens the CPU time involved during the agent Collect and Send Properties function.
17. **Issue:** With certain Access Protection rules enabled, VirusScan Enterprise was failing to return information to the Checkpoint SecureClient software. (Reference: 444667)  
**Resolution:** The binaries for Checkpoint integration have been updated to properly request information from VirusScan Enterprise.
18. **Issue:** Attempting to start an on-demand scan via the VirusScan tray icon could result in an error on Microsoft Windows Vista. (Reference: 446950)  
**Resolution:** The VirusScan tray icon correctly calls the on-demand scanner on User Access Controlled operating systems.
19. **Issue:** Creating a McAfee Installation Designer change package for VirusScan Enterprise and the AntiSpyware Enterprise Module, sometimes failed to upgrade the evaluations to licensed versions, for both products. (Reference: 437509)  
**Resolution:** McAfee Installation Designer configuration applicator upgrades the licenses of VirusScan Enterprise and the AntiSpyware Enterprise Module when they are both evaluations.
20. **Issue:** The VirusScan Console On-Delivery Email Scanner entry was not worded correctly in German. (Reference: 438931)  
**Resolution:** The VirusScan Resource file updates the displayed text to the correct wording in German.
21. **Issue:** One of the ScriptScan "McLogEvent" entries was always recorded in English. (Reference: 431071)  
**Resolution:** The Announcer library was updated to remove the extra notification.
22. **Issue:** In some cases, VirusScan Enterprise was not properly displaying Patch information about itself and currently installed VirusScan Modules\*. (Reference: 456826)  
**Resolution:** The VirusScan Management Plug-in has been updated to gather the current information about Patch levels of its installed VirusScan Modules\*.
23. **Issue:** When there were HotFixes or Patches available for the VirusScan Modules\*, they were not being downloaded to the clients. (Reference: 445494)  
**Resolution:** The AutoUpdate binary was modified to check for the existence of the VirusScan Module\* licenses when deciding which HotFixes or Patches to install.
24. **Issue:** Script errors were seen when attempting to view the Japanese text, of the product description window, in ePolicy Orchestrator 3.6.x. (Reference: 434203)  
**Resolution:** The VirusScan 8.7i NAP file has been updated to display the Japanese page in its proper Unicode format (UTF-8).
25. **Issue:** The alert options for Network Appliance Filer and ICAP scanners were visible on the workstation ePolicy Orchestrator policies. (Reference: 448361)  
**Resolution:** The VirusScan 8.7i NAP and extension have been updated to remove the alert options for alert options for Network Appliance Filer and ICAP scanners, from the workstation policy, as those scanners are server specific.
26. **Issue:** Some ePolicy Orchestrator operational events were not being generated for the VirusScan Modules\*. (Reference: 434423)  
**Resolution:** The VirusScan Reports extension updates the current VirusScan Enterprise Event IDs (1329 – 1339) to be used for the VirusScan Modules\*.
27. **Issue:** The on-demand scan log file validation checked for invalid file characters, including the "<" and ">" characters. (Reference: 433776)  
**Resolution:** The VirusScan 8.7i extension validation for the path name of the on-demand scanner log file now allows the "<" and ">" characters, which are needed for ePolicy Orchestrator macro variables.

28. **Issue:** The alert options for the VirusScan Modules\* would not gray out when inheritance was enforced on the parent policy. (Reference: 434231)  
**Resolution:** The VirusScan 8.7i NAP now properly enforces inheritance on the VirusScan Module alert options.
29. **Issue:** Events generated by the VirusScan Enterprise for Offline Virtual Images 1.0 software were not being generated in ePO reports. (Reference: 439832)  
**Resolution:** The McAfee Announcer library changed properties of the events to support current reporting in ePolicy Orchestrator 3.6.1.
30. **Issue:** Scanning events generated by VirusScan Enterprise 8.7i were not populating the Task Name with proper information. (Reference: 453515)  
**Resolution:** The McAfee Announcer library now populates the Task Name with the scanner that generated the event.
31. **Issue:** The Access Protection includes and exclude fields permitted a limited number of characters in the extension interface. (Reference: 457418/457419)  
**Resolution:** The VirusScan 8.7i extension updates the maximum limit of the include and exclude fields, to be consistent with the point-product interface.
32. **Issue:** Scanner exclusions that were entered in ePolicy Orchestrator with a preceding blank space did not show up correctly when they were enforced on the client. (Reference: 457420)  
**Resolution:** The VirusScan 8.5i extension has been updated to strip any preceding blank spaces from exclusions when they are entered in ePolicy Orchestrator.
33. **Issue:** VirusScan Enterprise added some new events that were not included in the default event filter, which was provided by ePolicy Orchestrator. (Reference: 462927)  
**Resolution:** The VirusScan Reports extension updates the current list to allow filtering of these events.

## Patch Inventory

This release consists of a package called VSE87P2.zip, which contains the following files:

Filename	Description
DEFERRED.MFE	MSI deferred action file
PKGCATALOG.Z	Package catalog file
PATCH2.HTM	This text file
VSE870DET.MCS	ePolicy Orchestrator detection script for VirusScan Enterprise
SETUP.EXE	Installer for this release
SETUP.INI	Initialization file for SETUP.EXE
PATCH2.MSP	Microsoft Installer Patch file
VSE870.NAP	ePolicy Orchestrator 3.6.x NAP for VirusScan Enterprise
VIRUSCAN8700.ZIP	ePolicy Orchestrator 4.x extension for VirusScan Enterprise
VIRUSCANREPORTS.ZIP	ePolicy Orchestrator 4.x Reports for VirusScan Enterprise

The following files are new with this Patch release:

Filename	Version
LOGPARSER.EXE	1.2.0.136
MIDUTIL.DLL	8.7.0.133
FTCFG.DLL	8.7.0.659
MCUPDATE.EXE	8.7.0.659
NAIANN.DLL	8.7.0.659
NCDAEMON.EXE	8.7.0.659
NCEXTMGR.EXE	8.7.0.659

NCINSTALL.EXE	8.7.0.659
NCMENU.EXE	8.7.0.659
NCSCAN.EXE	8.7.0.659
NCTRACE.EXE	8.7.0.659
QUARCPL.DLL	8.7.0.659
SCAN32.EXE	8.7.0.659
SCAN64.EXE	8.7.0.659
SHCFG32.EXE	8.7.0.659
VSUPDATE.DLL	8.7.0.659
BBCPL.DLL	8.7.0.747
COPTCPL.DLL	8.7.0.747
EMCFCGPL.DLL	8.7.0.747
MCAVDETECT.DLL	8.7.0.747
SCNCFG32.EXE	8.7.0.747
SHUTIL.DLL	8.7.0.747
VSODSCPL.DLL	8.7.0.747
VSPLUGIN.DLL	8.7.0.747
VSUPDCPL.DLL	8.7.0.747
SHSTAT.DLL	8.7.0.767
SHSTAT.EXE	8.7.0.767
VSTSKMGR.EXE	8.7.0.767
ADSLOKUU.DLL	14.1.0.515
CSSCAN.EXE	14.1.0.515
ENGINESERVER.EXE	14.1.0.515
ENTVUTIL.EXE	14.1.0.515
FTL.DLL	14.1.0.515
LOCKDOWN.DLL	14.1.0.515
MCSHIELD.DLL	14.1.0.515
MCSHIELD.EXE	14.1.0.515
MCSHIELDPERFDATA.DLL	14.1.0.515
MCVSSNMP.DLL	14.1.0.515
MFEANN.EXE	14.1.0.515
MYTILUS3.DLL	14.1.0.515
MYTILUS3_SERVER.DLL	14.1.0.515
MYTILUS3_SERVER_PROCESS.EXE	14.1.0.515
MYTILUS3_WORKER.DLL	14.1.0.515
NAEVENT.DLL	14.1.0.515
NAIEVENT.DLL	14.1.0.515
OTLKSCAN.DLL	14.1.0.515
OTLKUI.DLL	14.1.0.515
SCRIPTFF.DLL	14.1.0.515
SCRIPTSN.DLL	14.1.0.515
MFEAPFA.DLL	14.1.0.614
MFEAPFK.SYS	14.1.0.614
MFEAVFA.DLL	14.1.0.614
MFEAVFK.SYS	14.1.0.614
MFEBOPK.SYS	14.1.0.614
MFEHIDA.DLL	14.1.0.614

MFEHIDIN.EXE	14.1.0.614
MFEHIDK.SYS	14.1.0.614
MFERKDA.DLL	14.1.0.614
MFERKDET.SYS	14.1.0.614
MFETDIK.SYS	14.1.0.614
MFEVTPA.DLL	14.1.0.614
MFEVTPS.EXE	14.1.0.614
VSCAN.BOF	422
STRINGS.BIN	N/A
VSEVNTUI.DLL	N/A
VIRUSCAN8700.ZIP	8.7.0.170
VIRUSCANREPORTS.ZIP	1.1.0.145

## Installation Instructions

- To use this release, you must have VirusScan Enterprise 8.7i software installed on the computer you intend to update with this release.
- This release does not work with earlier versions of VirusScan software.
- A reboot is needed to fully load the system drivers into memory. The package installation does not force the reboot.

### Installation steps

1. Extract the Patch files from VSE87P2.zip to a temporary folder on your hard drive.
2. Double-click the file SETUP.EXE inside the temporary folder created in Step 1.
3. Follow the instructions of the installation wizard.

### Installation steps via ePolicy Orchestrator 3.6.x

1. On the computer where the ePolicy Orchestrator 3.x console resides, extract the Patch files and folders from VSE87P2.zip to a temporary folder on your hard drive.
2. Open the ePolicy Orchestrator 3.x console and add the package from the temporary folder created in Step 1 to your repository.  
**NOTE:** Refer to *Checking in Package* in the ePolicy Orchestrator 3.x online Help, or *Checking in PKGCATALOG.Z product packages* to the master repository in the ePolicy Orchestrator 3.6 online Help, for instructions on adding a package to the repository. The package type for this Patch is "Products or Updates."
3. The next time an agent update task runs, the VirusScan Enterprise client automatically downloads and installs the Patch.
4. In the ePolicy Orchestrator console, add the VSE870.NAP file using the Check in NAP wizard.  
**NOTE:** There is no new VSE870Reports.NAP with this Patch.

### Installation steps via ePolicy Orchestrator 4.x

1. On the computer where the ePolicy Orchestrator 4.x console resides, place the Patch archive VSE87P2.zip in a temporary folder on your hard drive.
2. Open the ePolicy Orchestrator 4.x console and add the VSE87P1.zip package from the temporary folder created in Step 1 to your repository.  
**NOTE:** Refer to *Checking in Packages Manually* in the ePolicy Orchestrator 4.x online Help, for instructions on adding a package to the repository. The package type for this Patch is "Products or Updates (.ZIP)."
3. The next time an agent update task runs, the VirusScan Enterprise client automatically downloads and installs the Patch.
4. From the top menu of the ePolicy Orchestrator console, click "Configuration."
5. From the menu tabs, click Extensions, then click Install Extensions in the lower left of the window.
6. Click Browse and locate the VIRUSCAN8700.zip extension update from the temporary folder created in Step 1.
7. Click OK to begin the extension update.
8. Repeat the checkin process for the VIRUSCANREPORTS.zip reports extension  
**NOTE:** Once the extensions are updated, the version can be verified in the ePolicy Orchestrator Extensions list (see *About this release* for version information).

## **HotFix and Patch reporting**

There is HotFix/Patch information in the ePolicy Orchestrator properties for each computer. On the ePolicy Orchestrator Properties tab for each computer, the VirusScan 8.7i General branch displays two entries:

- Patch – Displays the current Patch installed.
- Fixes - Displays any number of HotFixes listed in the registry.

A check is involved to verify that the HotFix/Patch matches the entry in the registry to the private build description of the binary. If the two don't match, the Patch or HotFix does not appear.

**NOTE:** Currently there are no reports or compliance checks that use this information.

## **Verifying installation**

Always reboot prior to validating that a Patch has been installed successfully.

1. Open the VirusScan Console and select About from the Help menu. The About VirusScan Enterprise window, Installed Patches, displays "1."
2. After property information has been collected by ePolicy Orchestrator agents, the client systems show that Patch 1 is installed as the "Hotfix" version. If the value HotfixVersions appears, it is a temporary value and is removed after a full property collection from the client.
3. Confirm that the expected files are installed by checking the version number of individual files. File versions should match the list of files in Patch Inventory, above.

**NOTE:** Patch releases do not display or report that the Patch is installed if an error occurred during installation, or if a file or files did not install correctly.

## **Removing the Patch**

Windows Installer 3.x and later now support the rolling back of Patches. This can be done one of two ways.

- For Windows XP, Windows 2003, Windows Vista, Windows 2008, and Windows 7 operating systems, the Patch can be removed manually via Add/Remove Programs if the user has administrative rights to the local system.
- For all operating systems that support Windows Installer 3.x, a command-line option can be used to remove the Patch silently.

### **Example:**

```
C:\WINDOWS\system32\Msixexec.exe /I {147BCE03-C0F1-4C9F-8157-6A89B6D2D973} MSIPATCHREMOVE={3E97AC3D-F01B-4BDC-887D-6F78CAF5F629} /q
```

### **Considerations**

1. The GUID information used here changes from one Patch to another. Always use the information in the Release Notes for the Patch that you are removing.
2. Because the Patch is removed via MSIEXEC, the functions inside setup.exe, which normally prevent reboots from occurring during silent processes, are not executed. In order to prevent a possible automatic reboot from occurring after a Patch removal, simply add the REBOOT=R parameter to the command-line option above.
3. Patch removal is an MSI reinstall function. When a Patch is removed, all features affected by the Patch are reset to installation defaults. Any features not modified by the Patch are left with their current settings.
4. Update VirusScan after removing the Patch to ensure that the latest versions of the engine and DAT files are run.

## **License attributions**

This product includes or may include:

Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). | Cryptographic software written by Eric A. Young and software written by Tim J. Hudson | Some software programs

that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.

\* Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. | Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. | Software written by Douglas W. Sauder. | Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at [www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt). | International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. | Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. | FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany. | Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc. | Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. | Software copyrighted by Expat maintainers. | Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000. | Software copyrighted by Gunnar Ritter. | Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003. | Software copyrighted by Gisle Aas. © 1995-2003. | Software copyrighted by Michael A. Chase, © 1999-2000. \* Software copyrighted by Neil Winton, © 1995-1996. | Software copyrighted by RSA Data Security, Inc., © 1990-1992. | Software copyrighted by Sean M. Burke, © 1999, 2000. | Software copyrighted by Martijn Koster, © 1995. | Software copyrighted by Brad Appleton, © 1996-1999. | Software copyrighted by Michael G. Schwern, © 2001. | Software copyrighted by Graham Barr, © 1998. | Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. | Software copyrighted by Frodo Looijaard, © 1997. | Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at [www.python.org](http://www.python.org). | Software copyrighted by Beman Dawes, © 1994-1999, 2002. | Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. | Software copyrighted by Simone Bordet & Marco Cravero, © 2002. | Software copyrighted by Stephen Purcell, © 2001. | Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). | Software copyrighted by International Business Machines Corporation and others, © 1995-2003. | Software developed by the University of California, Berkeley and its contributors. | Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod\_ssl project (<http://www.modssl.org/>). | Software copyrighted by Kevlin Henney, © 2000-2002. | Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. | Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. | Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. | Software copyrighted by Boost.org, © 1999-2002. | Software copyrighted by Nicolai M. Josuttis, ©1999. | Software copyrighted by Jeremy Siek, © 1999-2001. | Software copyrighted by Daryle Walker, © 2001. | Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. | Software copyrighted by Samuel Krempf, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. | Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. | Software copyrighted by Cadenza New Zealand Ltd., © 2000. | Software copyrighted by Jens Maurer, © 2000, 2001. | Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. | Software copyrighted by Ronald Garcia, © 2002. | Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. | Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. | Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. | Software copyrighted by Paul Moore, © 1999. | Software copyrighted by Dr. John Maddock, © 1998-2002. | Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. | Software copyrighted by Peter Dimov, © 2001, 2002. | Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. | Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002. | Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992. | Software copyrighted by Cambridge Broadband Ltd., © 2001-2003. | Software copyrighted by Sparta, Inc., © 2003-2004. | Software copyrighted by Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. | Software copyrighted by Simon Josefsson, © 2003. | Software copyrighted by Thomas Jacob, © 2003-2004. | Software copyrighted by Advanced Software Engineering Limited, © 2004. | Software copyrighted by Todd C. Miller, © 1998. | Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

## COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

## TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX

(MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

## LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.